?b wpi

30jun00 12:08:25 User212334 Session D2250.1
Sub account: P001249
$0.00 0.162 DialUnits FileHomeBase
$0.00 Estimated cost FileHomeBase
$0.11 TYMNET
$0.11 Estimated cost this search
$0.11 Estimated total session cost 0.162 DialUnits

File 351:DERWENT WPI 1963-2000/UD=, UM=, & UP=200030
(c) 2000 Derwent Info Ltd
***File 351: Display format changes now online.**
Please see HELP NEWS 351 for details.

Set	Items	Description
?s pn=de 4325459		
S1	1	PN=DE 4325459

?t s1/5

1/5/1
DIALOG(R)File 351:DERWENT WPI
(c) 2000 Derwent Info Ltd. All rts. reserv.

010174342 **Image available**
WPI Acc No: 1995-075595/**199511**
XRPX Acc No: N95-060017
Multitone generator for cryptographic identification and authorisation to access telephone banking system - has generator with ROM and EEPROM memories contg. secret access code, and output to loudspeaker for telephone input
Patent Assignee: C2S GMBH CRYPTOGRAFISCHE SICHERHEITSSYST (CTWO-N)
Inventor: EISELE R H
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 4325459	A1	19950209	DE 4325459	A	19930729	199511	B

Priority Applications (No Type Date): DE 4325459 A 19930729
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 4325459	A1		9	H04L-009/32	

Abstract (Basic): DE 4325459 A
The signal generator controls access for the link between a customer and a central computer. A box (1) has a multi-tone selector keyboard (3) and a series of function keys (4).
Internally the unit has ROM and EEPROM integrated into a single chip, with the contents containing a secret code value for access. Signal output is to a loudspeaker (7) that fits over the mouthpiece of a telephone.
USE - Controls access to telephone banking systems, or ordering of cheque books.
Dwg.2a/4
Title Terms: MULTITONE; GENERATOR; CRYPTOGRAPHIC; IDENTIFY; AUTHORISE; ACCESS; TELEPHONE; BANK; SYSTEM; GENERATOR; ROM; EEPROM; MEMORY; CONTAIN; SECRET; ACCESS; CODE; OUTPUT; LOUDSPEAKER; TELEPHONE; INPUT
Derwent Class: T01; T05; W01

International Patent Class (Main): H04L-009/32
International Patent Class (Additional): G06F-012/14; G06F-013/00;
G07F-019/00; H04L-027/26; H04M-011/06
File Segment: EPI

98P 1245

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 43 25 459 A 1**

B1

(51) Int. Cl.[6]:
H 04 L 9/32
G 06 F 13/00
G 07 F 19/00
G 06 F 12/14
H 04 L 27/26
H 04 M 11/06

(21) Aktenzeichen: P 43 25 459.4
(22) Anmeldetag: 29. 7. 93
(43) Offenlegungstag: 9. 2. 95

DE 43 25 459 A 1

(71) Anmelder:
C2S GmbH Cryptografische SicherheitsSysteme, 65510 Idstein, DE

(74) Vertreter:
Leineweber, J., Dipl.-Phys., Pat.-Anw., 50859 Köln

(72) Erfinder:
Eisele, Raymund H., 65510 Idstein, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Tongeber mit Identifikations- und Authentisierungs-Einrichtung

(57) Die Erfindung betrifft eine Vorrichtung (1) mit einem Mehrfrequenz-Tongeber (10), einer numerischen Tastatur (3), Funktionstasten (4), einem Bildschirm (2), einem Prozessor (12) mit Rom-Speicher (14) und EEPROM-Speicher (13) sowie Input- (15) und Output-Treibern (16) sowie einem Verschlüsselungsverfahren zur sicheren Identifikation eines Benutzers, wenn dieser sich z. B. über eine Telefonleitung gegenüber einem Zentralrechner ausweist und einem Verfahren zur Errechnung eines Nachrichtenechtheits-Codes zur Absicherung von Überweisungen gegen unerkannte Veränderung während der Übertragung vom Benutzer zu einer entfernt stehenden EDV-Einrichtung.

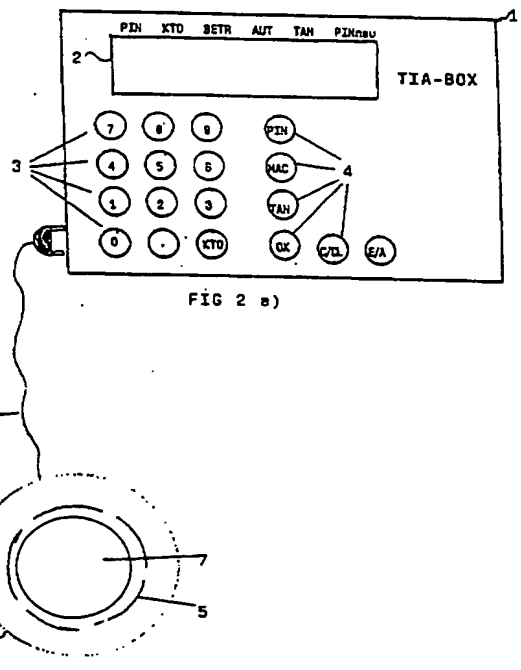


FIG 2 a)

DE 43 25 459 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 12. 94 408 066/45

Beschreibung

Die meisten Telefone arbeiten nach dem Impulswahlverfahren (IWV), damit können über die Wählscheibe oder die Wähltastatur keine "Daten" zur Weiterleitung über die Telefonleitung eingegeben werden. Um solche "Daten" über die Telefonleitung zu senden, ist das Mehrfrequenzverfahren (MFV) notwendig. Um z. B. einen Anrufbeantworter über eine Fernabfrage zu bedienen, gibt es Codesender, die mit einer numerischen Tastatur und Funktionstasten ausgestattet sind und auf die Sprechmuschel des Telefonhörers gehalten werden. Wenn eine Taste der Tastatur gedrückt wird, wird ein Ton nach dem Mehrfrequenzverfahren erzeugt. Dieser wird z. B. von dem Anrufbeantworter als ein Befehl interpretiert.

Es gibt auch Verschlüsselungsgeräte in der Form eines Taschenrechners, die nach dem sogenannten Challenge/Response-Verfahren arbeiten. Das Verschlüsselungsgerät wird aktiviert, indem die Persönliche Identifikations-Nummer (PIN) des Benutzers eingegeben wird. Danach meldet sich der Benutzer bei einem entfernt stehenden System (z. B. EDV-Anlage) mit seiner Benutzer-Nummer an. Um die Berechtigung für den Zugang zu dem entfernt stehenden System durch dieses zu überprüfen, wird dem Benutzer eine Zufallszahl (meistens 8-stellig) gesendet. Diese Zufallszahl (Challenge) gibt der Benutzer in sein Verschlüsselungsgerät ein, dort wird sie verschlüsselt und als Antwort wird die Response-Nummer angezeigt. Diese Response-Nummer übermittelt der Benutzer an das entfernt stehende System zur Überprüfung. In dem entfernt stehenden System wird eine Response-Nummer nach demselben Algorithmus erzeugt. Wenn die so erzeugte Response-Nummer mit der vom Benutzer erhaltenen übereinstimmt, ist sichergestellt, daß es sich um einen berechtigten Benutzer handelt.

Bekannt sind auch das AIDA-System aus dem USA-Patent Nr. 4,849,613 und das PASS-System sowie die PASS-Methode aus dem Tagungsband DATASAFE 2. Int. Fachmesse und Kongreß für Datensicherheit, 26.—28. Nov. 1991 Seite 73 ff., erschienen im vde-verlag gmbh, Berlin und Offenbach ISBN 3-8007-1821-9, dabei handelt es sich auch um ein Verschlüsselungsgerät in der Form eines Taschenrechners. Die PASS-Methode arbeitet jedoch nicht nach dem Challenge/Response-System sondern nach dem Session-PIN-System. Dabei wird das Verschlüsselungsgerät durch die Eingabe einer PIN aktiviert, als Antwort wird eine sogenannte Session-PIN angezeigt, die für jede Verbindung (Session) aufgrund von sich ständig ändernden Geheimwerten neu errechnet wird.

Seit einiger Zeit bieten Kreditinstitute ihren Kunden einen Service an, der allgemein als Telephone Banking oder als KONTOFON bekannt ist. Dabei erhält der Kunde die Möglichkeit, über das Telefon z. B. seinen Kontostand abzufragen, Überweisungen aufzugeben, Schecks zu bestellen oder Daueraufträge zu ändern. Auf der Seite des Kreditinstituts sitzen Mitarbeiter am Telefon und nehmen die Aufträge entgegen. Um einem Kunden seinen Kontostand mitzuteilen, müssen die Mitarbeiter des Kreditinstituts zunächst prüfen, ob es sich um einen berechtigten Kunden handelt. Das wird üblicherweise durch das Erfragen der Kontonummer und eines Paßwortes durchgeführt. Diese Paßworte sind statisch und werden im Klartext über die Telefonleitung übertragen. Daß das zu Mißbrauch führen kann, ist offensichtlich. Wenn Überweisungsaufträge an eine Bank gegeben werden, müssen diese vom Kunden unterschrieben werden. Beim Telephone Banking ist dies heute nicht möglich, deshalb werden von den Kreditinstituten Betragsobergrenzen festgesetzt. Für eventuelle Fehlausführungen haftet üblicherweise der Kunde aufgrund der speziellen Allgemeinen Geschäftsbedingungen. Das gleiche gilt auch bei der Benutzung von Bildschirmtext. Dort werden zwar Überweisungen mit einer sogenannten TAN (Transaktionsnummer) gesichert, diese schützt jedoch nicht gegen die Veränderung des Inhalts der Überweisung.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, die Identifikation eines Kunden im Rahmen von Telephone Banking, Bildschirmtext oder ähnlichen Anwendungen kryptographisch sicher durchzuführen, den Inhalt von Überweisungen gegen absichtliche oder zufällige Veränderung während der Übertragung kryptographisch zu sichern und andere Transaktionen, wie z. B. das Bestellen von Scheckformularen durch einen Zusatzcode zu sichern. Dabei wird besonderer Wert darauf gelegt, daß das Sicherheits-System nicht nur sicher, sondern vom Kunden leicht zu handhaben ist und auf Seiten z. B. der Kreditinstitute der gesamte Vorgang ohne Einsatz von Personen durchgeführt werden kann.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, daß der Kunden eine Tongeber mit Identifikations- und Authentisierungs-Einrichtung (TIA-Box) erhält, die von dem Kreditinstitut personalisiert wurde (mit für nur diesen Kunden gültigen Geheimwerten geladen wird). Diese TIA-Box hat das äußere Aussehen eines Taschenrechners mit numerischen Tasten, Funktions-Tasten, einem Bildschirm und einem Tongeber mit Lautsprecher nach dem Mehrfrequenzverfahren. Ferner enthält die TIA-Box eine oder mehrere Batterien oder eine Solarzelle und neben anderen elektronischen Bauteilen einen Prozessor mit ROM und EEPROM-Speicher. Im ROM-Speicher sind der Verschlüsselungs-Algorithmus, das Schlüsselverwaltungssystem, ein sogenannter Initialisierungs-Schlüssel sowie Software zur Bedienerführung und Ein-/Ausgabefunktionen enthalten. Der Verschlüsselung-Algorithmus und das Schlüsselverwaltungssystem werden als PASS-Methode bezeichnet. Im EEPROM-Speicher werden die Kontonummer oder Stamm-Nummer des Kunden und wahlweise seine Bankleitzahl sowie die variablen Geheimwerte gehalten, die sich nach jedem Durchlauf des Algorithmus ändern. Es ist auch möglich, daß die TIA-Box mit einem Chipkartenleser versehen wird, um die Geheimwerte nicht aus dem EEPROM-Speicher der TIA-Box zu lesen, sondern von der Chipkarte. Der Lautsprecher der TIA-Box kann wahlweise auf der Rückseite der TIA-Box angebracht sein, dann muß diese während der Übertragung der Daten an die Sprechmuschel des Telefonhörers gehalten werden oder der Lautsprecher kann sich in einer separaten Einrichtung befinden, die wahlweise mit einem Saugknopf an der Sprechmuschel befestigt oder an diese gehalten wird und mit der TIA-Box über ein Kabel oder schnurlos kommuniziert. Sowohl die TIA-Box als auch die separate Einrichtung können mit Schlitzen versehen werden, so daß, obwohl sich die jeweilige Einrichtung vor der Sprechmuschel befindet, trotzdem Sprechimpulse über das Telefon übertragen werden können.

Eine typische Anwendung im Telephone Banking sieht beim Einsatz der TIA-Box folgendermaßen aus:
Nachdem der Kunde das Kreditinstitut über das Telefon angewählt hat, wird er z. B. über eine Sprachausgabeeinrichtung aufgefordert, sich auszuweisen. Dazu gibt

der Kunde seine selbst gewählte Geheimzahl in die TIA-Box ein und betätigt die Funktionstaste "OK"-Taste. Dabei werden aus dem EEPROM-Speicher der TIA-Box die Kontonummer (Stammnummer) und wahlweise die Bankleitzahl über den Tongeber an den Lautsprecher und von dort über die Telefonleitung an das Kreditinstitut übertragen. Ferner wird mit Hilfe der PASS-Methode und der Geheimwerte des Kunden, die im EEPROM-Speicher abgelegt sind, ein einmalig verwendbarer Identifikations-Code erzeugt und über das Telefon an das Kreditinstitut übertragen. Dort wird [redacted] und den dort verschlüsselt gespeicherten Geheimwerten dieses Kunden der Identifikations-Code überprüft. Wenn er übereinstimmt, ist sichergestellt, daß es sich um einen berechtigten Kunden handelt.

Wenn der Kunde z. B. aufgrund eines Auswahlmenues der Sprachausgabe Scheckformulare bestellen möchte, wird er aufgefordert, auf seiner TIA-Box die Funktion-Taste "TAN" und danach die "OK"-Taste" zu drükken. Von der PASS-Methode wird dann eine TAN (Transaktions-Nummer) generiert und an das Kreditinstitut zur Überprüfung übertragen.

Will der Kunde z. B. eine Überweisung ausführen, wird er aufgefordert, in die TIA-Box, nachdem er die Funktions-Taste "MAC" (Message Authentication Code) gedrückt hat, die Kontonummer und die Bankleitzahl des Empfängers einzugeben und die "OK"-Taste zu betätigen. Das EDV-System des Kreditinstituts prüft nun, ob unter dieser Bankleitzahl und Kontonummer bereits ein Eintrag im Sprachspeicher vorhanden ist. Wenn ein Eintrag gefunden wurde, wird der Empfängername über die Sprachausgabe an den Kunden mitgeteilt. Wenn der Empfängername richtig ist, bestätigt der Kunde dies indem er die "OK"-Taste betätigt. Wurde kein Empfängername gefunden, wird der Kunde gebeten, den Empfängernamen mündlich bekanntzugeben. Er wird im EDV-System des Kreditinstituts als Sprachaufzeichnung gespeichert und muß bei der Nachbearbeitung manuell zu der Überweisung zugefügt werden. Der Empfängername wird dem Kunden nochmals "vorgelesen" und wenn er richtig ist, bestätigt es der Kunde durch das Betätigen der "OK"-Taste. Als nächstes wird er gebeten, den Betrag in die TIA-Box einzugeben und die "OK"-Taste zu drücken. Für die Angabe des Verwendungszwecks erhält der Kunde von der Sprachausgabe ein weiteres Auswahlmenue. Er wählt mit einer numerische Taste der TIA-Box den gewünschten Verwendungszweck aus und ergänzt ihn evtl. um z. B. Rechnungs- oder Mitgliedsnummer. Wenn alle Daten richtig erfaßt sind, wird der Kunde von der Sprachausgabe gebeten, die "MAC"-Taste zu drücken. Aus den Werten Kontonummer des Empfängers, evtl. Bankleitzahl des Empfängers und dem Betrag, die während der Eingabe im EEPROM-Speicher zwischengespeichert wurden, wird mit der PASS-Methode ein MAC (Nachrichtenechtheits-Code) errechnet und an das Kreditinstitut übertragen. Dort wird er mit der PASS-Methode nachgeprüft. Wenn er übereinstimmt, ist sichergestellt, daß die eingegebenen Werte während der Übertragung nicht unerkannt verändert wurden und daß die Überweisung von einem berechtigten Kunden stammt.

Es ist auch möglich, die TIA-Box für Btx-Anwendungen oder für Telephone Banking mit bestimmten Telefonapparaten, die zwar nach dem Impulswahlverfahren die Anwahl durchführen, aber danach durch eine bestimmte Tastenkombination auf das Mehrfrequenzverfahren umgestellt werden können. In diesen Fällen wird die TIA-Box als reiner Verschlüsselungsrechner eingesetzt. Zur Identifikation des Kunden gibt er seine PIN in die TIA-Box ein, als Antwort erhält er eine Session-PIN. Diese gibt er zusammen mit seiner Konto-Nummer in sein Btx-Gerät oder über die Tastatur seines Telefonapparates ein. Bei Überweisungen wird die Überweisung am Btx-Gerät oder der Telefon-Tastatur erfaßt. Zur Absicherung z. B. der Konto-Nummer des Empfängers und des Betrages werden diese Werte in die TIA-Box eingegeben, ein MAC errechnet und auf dem Bildschirm der TIA-Box angezeigt. Der angezeigte MAC wird in das Btx-Gerät oder die Telefon-Tastatur eingegeben und zum Nachprüfen an das EDV-System des Kreditinstituts übertragen. Wenn für eine Transaktion eine TAN benötigt wird, drückt der Kunde die "TAN"-Taste der TIA-Box, eine TAN wird angezeigt und vom Kunden in das Btx-Gerät oder die Telefon-Tastatur zur Übertragung an das Kreditinstitut und zur Überprüfung eingegeben.

Es zeigen:

Fig. 1.a) eine TIA-Box mit der erfindungsgemäßen Gestaltung als Verschlüsselungsgerät mit integriertem Lautsprecher, der Töne nach dem Mehrfrequenzverfahren aussendet.

Fig. 1.b) Rückseite einer TIA-Box

Fig. 2.a) eine TIA-Box mit der erfindungsgemäßen Gestaltung als Verschlüsselungsgerät mit einer separaten Einheit, die den Lautsprecher und die Öffnungsschlitze enthält.

Fig. 2.b) die Rückseite der separaten Einheit **8**, die wahlweise auch einen Saugnapf enthält, um diese Einheit an der Sprechmuschel eines Telefonhörers zu befestigen. Die separate Einheit ist in diesem Fall über ein Kabel und einen Stecker mit der TIA-Box verbunden.

Fig. 2.c) einen Querschnitt der separaten Einheit **8**, die auf der Außenseite eine umlaufende Vertiefung **18** enthält, um darin das Verbindungskabel zur TIA-Box aufzuwickeln.

Fig. 3. eine TIA-Box mit der Möglichkeit, eine Chipkarte einzustecken, um die Geheimwerte auf dieser abzulegen und von dieser auszulesen. Der in der TIA-Box integrierte Chipkarten-Leser ist nicht dargestellt.

Fig. 4. Schemazeichnung der elektronischen Komponenten mit deren Inhalten, wie sie in der TIA-Box vorhanden sind.

Die in **Fig.** 1.a) dargestellte TIA-Box **1** umfaßt einen Bildschirm **2**, der die Möglichkeit hat, unter den darüber aufgedruckten Bezeichnungen wie PIN, KTO, BETR, MAC, TAN, PINneu entweder blinkende Fragezeichen (?) oder Gleichheitszeichen darzustellen. Wird der Benutzer aufgefordert, seine PIN einzugeben, erscheint unter der Bezeichnung "PIN" ein blinkendes Fragezeichen. Der Zugangscode (Session-PIN) wird errechnet und angezeigt, indem unter der Bezeichnung "PIN" ein Gleichheitszeichen erscheint und in den rechten Stellen des Bildschirms die Session-PIN angezeigt wird.

Ferner sind numerische Tasten (3 von 0—9) sowie Funktions-Tasten **4** (PIN, MAC, TAN, KTO, OK, C/CE, on/off) dargestellt. Die Funktions-Tasten **4** haben folgende Funktionen:

PIN-Taste: Die Funktion PIN-Eingabe, Generieren Session-PIN und Ausgabe der Session-PIN wird gewünscht.

MAC-Taste: Die Eingabe von z. B. Überweisungsdaten und die Errechnung und Ausgabe eines Nachrichten-Echtheits-Code wird gewünscht.

TAN-Taste: Die Generierung und Ausgabe einer TAN wird gewünscht.

KTO-Taste: Die Anzeige der Kontonummer, für die

diese TIA-Box initialisiert wurde, wird gewünscht.

OK-Taste: Bestätigung-Taste zur Übertragung von Daten.

C/CE-Taste: Löschtaste

on/off-Taste: Taste zum Ein- und Ausschalten der TIA-Box.

Auf der rechten Seite der TIA-Box befinden sich Öffnungsschlitze 5 die es ermöglichen, durch die TIA-Box hindurchzusprechen.

Die in **Fig.** 1.b) dargestellte Rückseite der TIA-Box 1 umfaßt Öffnungsschlitze 5 die es ermöglichen, durch die TIA-Box hindurchzusprechen und einen Lautsprecher 7, der die MFV-Signale ausgibt.

Bei der in **Fig.** 2.a) dargestellten TIA-Box befinden sich der Lautsprecher und die Öffnungsschlitze in einer separaten Einheit 8, die über ein Verbindungskabel 9 oder über Funk/Infrarot mit der TIA-Box kommuniziert.

Bei der in **Fig.** 2.b) dargestellten Rückseite der separaten Einheit 8 befindet sich neben dem Lautsprecher und den öffnungsschlitzen wahlweise ein Saugnapf 10, der zur zeitweisen Befestigung der separaten Einheit 8 an der Sprechmuschel eines Telefonhörers (nicht dargestellt) dient.

Der in **Fig.** 2.c) dargestellte Querschnitt der separaten Einheit 8 zeigt eine rundum verlaufende Vertiefung 18, in die wahlweise das Verbindungskabel zur TIA-Box aufgewickelt werden kann.

Die in **Fig.** 3 dargestellte TIA-Box zeigt die Möglichkeit, eine Chipkarte 11 einzustecken. Über eine in der TIA-Box befindende Chipkarten Schreib-/Leseeinheit (nicht dargestellt) können die Geheimwerte eines Benutzers von der Chipkarte gelesen und die neu errechneten Geheimwerte darauf geschrieben werden.

Die in **Fig.** 4 dargestellten elektronischen Einheiten sind erforderlich, um die Funktionen der TIA-Box auszuführen. Im Prozessor 12 werden die Rechenvorgänge durchgeführt. Der ROM-Speicher 14 enthält die Verarbeitungs-Software sowie die PASS-Methode und einen Initialisierungs-Schlüssel. Im EEPROM-Speicher werden die veränderbaren Werte wie Kontonummer, Bankleitzahl, PIN, Faktor P, Faktor M und Session-Schlüssel gespeichert. Er dient auch als Zwischenspeicher für die Werte Empfänger-Kontonummer, Empfänger-Bankleitzahl und Überweisungs-Betrag. Sinnvollerweise werden die Einheiten Prozessor 12, ROM-Speicher 14 und EEPROM-Speicher in einem einzigen Chip integriert, damit die in den Speichern 13, 14 befindende Geheimwerte nicht während der Übertragung in den Prozessor "abgehört" werden können. Sollten die Speicher nicht in den Prozessor-Chip integriert sein, ist erforderlich, daß die Inhalte der Geheimwerte für die Speicherung verschlüsselt werden.

Die besonderen Vorteile der beschriebenen TIA-Box mit den integrierten Funktionen sind: Die bei den bestehenden Systemen wie z. B. Telephone Banking oder Home Banking über Bildschirmtext (Btx) oder DATEX-J bestehen erhebliche Sicherheitslücken wie z. B. sichere Identifikation des Kunden und Schutz der Informationen z. B. eines Überweisungsauftrags gegen zufällige oder absichtliche Veränderung während der Übertragung an das Kreditinstitut werden durch die Funktionen der TIA-Box beseitigt. Bei z. B. Telephone Banking bietet das TIA-System die großen Vorteile, daß der Kunde nur noch die variablen Werte einer Transaktion über die Tastatur der TIA-Box eingeben muß und diese automatisch gegen unerkannte Veränderung gesichert werden. Für den Kunden entfällt auch die Eingabe seiner Kontonummer und evtl. der Bankleitzahl. Das Kreditinstitut hat neben den Vorteilen, daß das TIA-System die Sicherheit wesentlich erhöht den weiteren Vorteil, daß bewährte Techniken der Sprachausgabe und der automatischen Erfassung der Eingabedaten eingesetzt werden können. Andere Möglichkeiten ohne das TIA-System wäre, daß Mitarbeiter den Dialog mit dem Kunden führen und die Informationen manuell erfassen müßten. Das ist sehr aufwendig. Auch an die Möglichkeit der Spracherkennung kann gedacht werden, dabei handelt es sich jedoch um ein System, das heute noch nicht unbedingt ausgereift ist.

Der Kunde, der eine TIA-Box hat, kann rund um die Welt seine Bankgeschäfte sicher per Telefon erledigen. Wenn er zusätzlich Btx benutzt, kann er dasselbe System mit der gleichen Sicherheit auch verwenden.

Patentansprüche

1. Verfahren zur Kommunikation mit einem Zentralrechner, wie Telephone Banking, Bildschirmtext oder ähnliche Anwendungen, **dadurch gekennzeichnet,** daß zur Datenübertragung zwischen dem Kunden und dem Zentralrechner das Mehrfrequenzverfahren angewendet wird.
2. Benutzerseitige Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1, dadurch gekennzeichnet, daß sie neben einer Mehrfrequenztongeber-Tastatur (3) eine personalisierte Identifikations- und Authentisierungs-Einrichtung umfaßt.
3. Vorrichtung nach Anspruch 2, dadurch gekennzeichnet, daß sie einen Prozessor (12) für die Durchführung der Rechenvorgänge, eine ROM-Speicher (14) und einen EEPROM-Speicher (13) enthält.
4. Vorrichtung nach Anspruch 3, dadurch gekennzeichnet, daß Prozessor (12), ROM-Speicher (14) und EEPROM-Speicher (13) ein einem einzigen Chip integriert sind.
5. Vorrichtung nach Anspruch 2, 3 oder 4, dadurch gekennzeichnet, daß eine Tongeber-Tastatur (3), die Identifikations- und Authentisierungs-Einrichtung, Funktionstasten (4) und ein Display (2) sowie wahlweise einen Lautsprecher (7), eine schreib- und/oder Leseeinheit für eine Chipkarte (11), eine Batterie (2) und oder eine Solarzelle Bestandteile einer Box (TIA-Box) sind, die das äußere Aussehen eines Taschenrechners hat.
6. Vorrichtung nach Anspruch 5, dadurch gekennzeichnet, daß der Lautsprecher (7) eine separate Einheit (10) ist, die entweder über ein Kabel oder über Funk/Infrarot mit der TIA-Box (1) kommuniziert.
7. Vorrichtung nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß TIA-Box (1) oder separate Einheit (10) mit einem Saugnapf (8) zur Befestigung an einem Telefonhörer ausgerichtet sind.
8. Vorrichtung nach Anspruch 5, 6 oder 7, dadurch gekennzeichnet, daß die separate Einheit (10 mit einer umlaufenden Vertiefung ausgerichtet ist, in die das Verbindungskabel aufgewickelt werden kann.
9. Vorrichtung nach Anspruch 5, 6, 7 oder 8, dadurch gekennzeichnet, daß TIA-Box (1) oder separate Einheit (10) mit Schlitzen ausgerüstet sind, die den Zugang von Sprachsignalen zum Mikrofon des Telefonhörers freihalten.
10. Vorrichtung nach einem der Ansprüche 2, 3

oder 4, dadurch gekennzeichnet, daß zumindest die Tongeber-Tastatur Bestandteil eines Telefon-Apparates ist, dessen numerische Tastatur als Mehrfrequenz-Tongeber benutzbar ist.

11. Vorrichtung nach Anspruch 10, dadurch gekennzeichnet, daß zumindest ein Teil der im Anspruch 5 aufgeführten Elemente Bestandteile des Telefon-Apparates oder des Bildschirmtext-Gerätes sind.

12. Verfahren zur Kommunikation mit einem Zentralrechner nach Anspruch 1 mit einer Vorrichtung nach einem der Ansprüche 2 bis 10, dadurch gekennzeichnet, daß die Verschlüsselung und Kommunikation nach der Challenge/Response- oder PASS-Methode durchgeführt wird.

13. Verfahren zur Benutzung eines Elements nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zur eindeutigen Identifikation eines Benutzers dessen Identifikations-Nummer aus dem Speicher des Elements ausgelesen sowie ein individueller Zugangs-Code generiert wird und an die entfernt stehende EDV-Einrichtung automatisch übertragen und dort automatisch erfaßt und nachgeprüft wird.

14. Verfahren zur Benutzung eines Elements nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die numerischen Werte einer Überweisung in das Element eingegeben werden, dort zwischengespeichert und gleichzeitig an eine entfernt stehende EDV-Einrichtung übertragen werden und zum Abschluß der Transaktion für die zwischengespeicherten Werte ein Nachrichtenechtheits-Code generiert und an die entfernt stehende EDV-Einrichtung zur Überprüfung übertragen wird.

15. Verfahren zur Benutzung eines Elements nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß durch das Drücken der TAN-Taste des Elements ein verbindungsabhängiger Pseudozufalls-Code generiert wird und an eine entfernt stehende EDV-Einrichtung zur Überprüfung übertragen wird.

16. Verfahren zur Benutzung eines Elements nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß nach der Eingabe der Persönlichen Identifikations-Nummer (PIN) des Benutzers dieser eine neue PIN eingeben kann, die in der Einheit gespeichert wird und ferner verschlüsselt an die entfernt stehende EDV-Einrichtung zur Speicherung übertragen wird.

Hierzu 4 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 43 25 459 A1
Int. Cl.6: H 04 L 9/32
Offenlegungstag: 9. Februar 1995

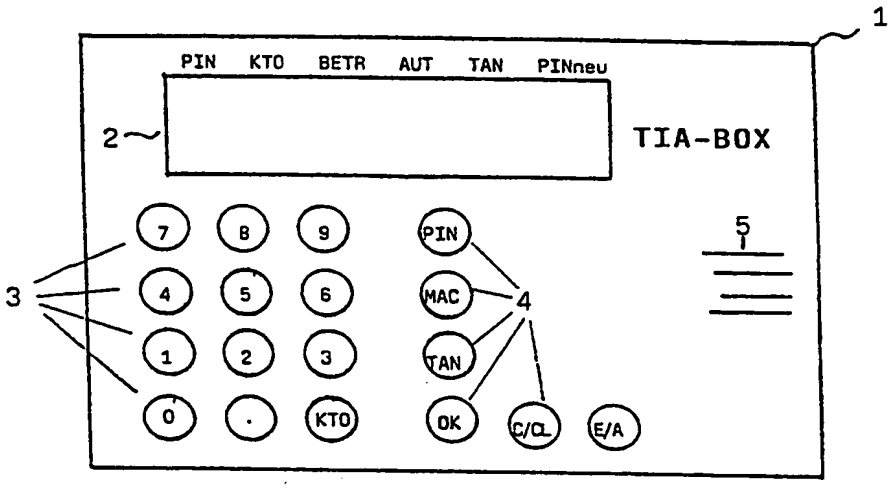


FIG. 1 a)

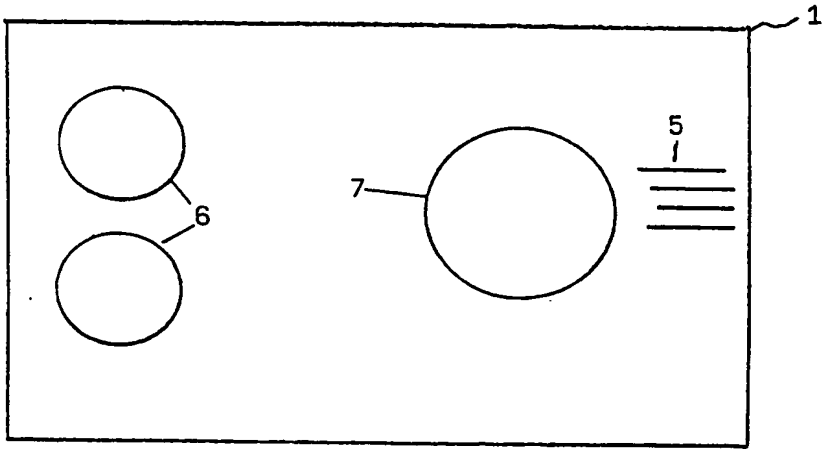


FIG. 1 b)

Nummer: DE 43 25 459 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 9. Februar 1995

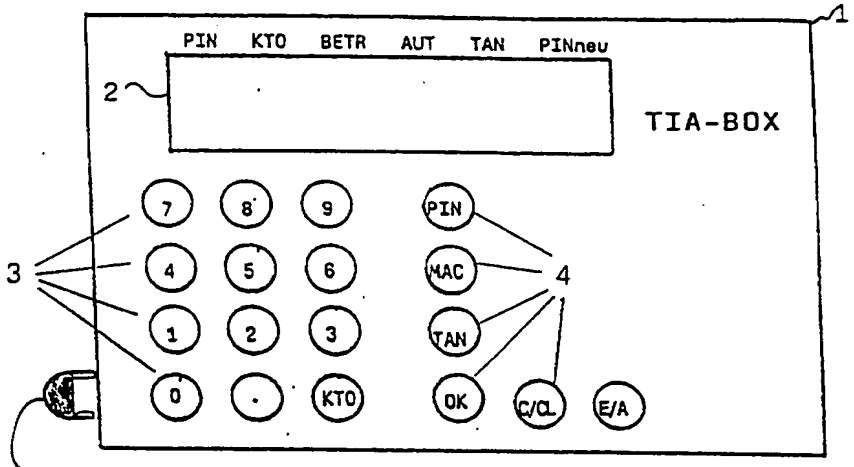
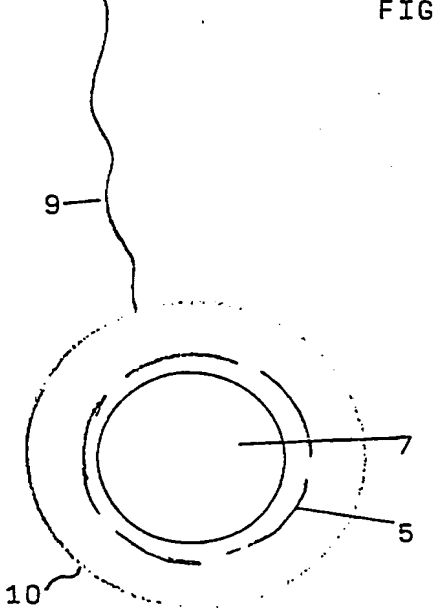


FIG 2 a)



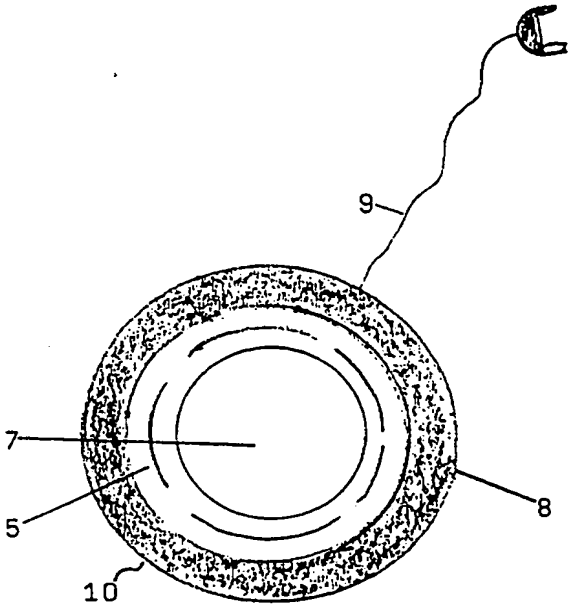


FIG. 2 b)

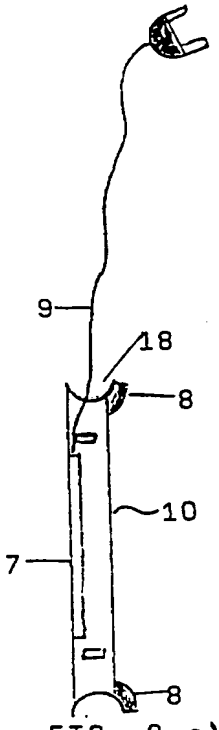


FIG. 2 c)

Nummer: DE 43 25 459 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 9. Februar 1995

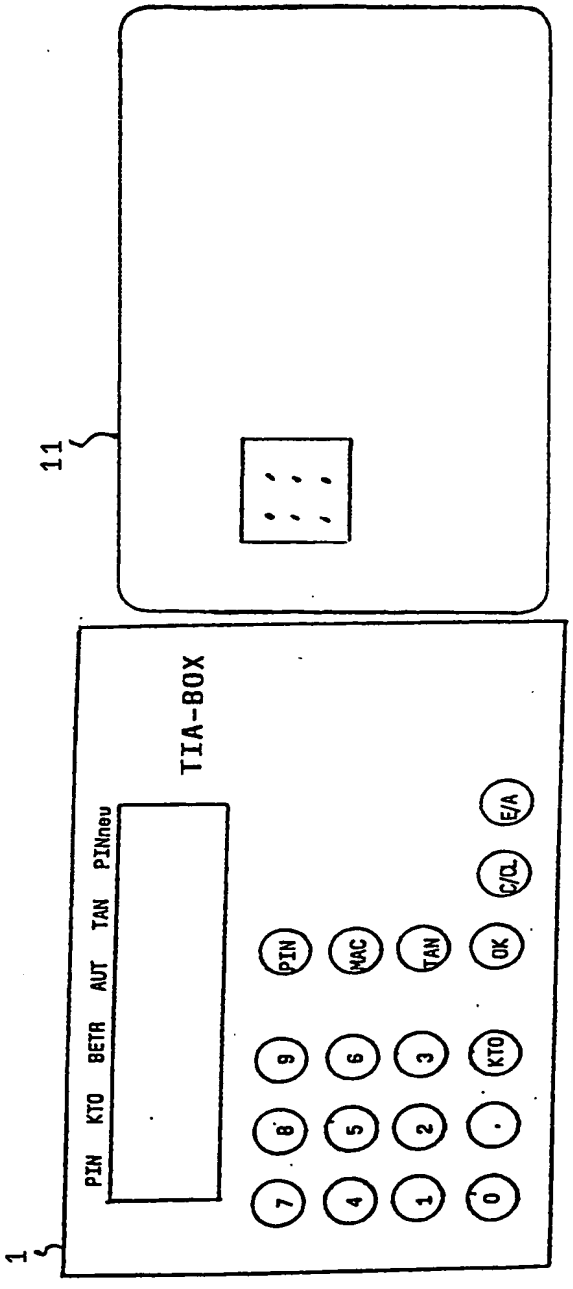


FIG. 3

Nummer: DE 43 25 459 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 9. Februar 1995

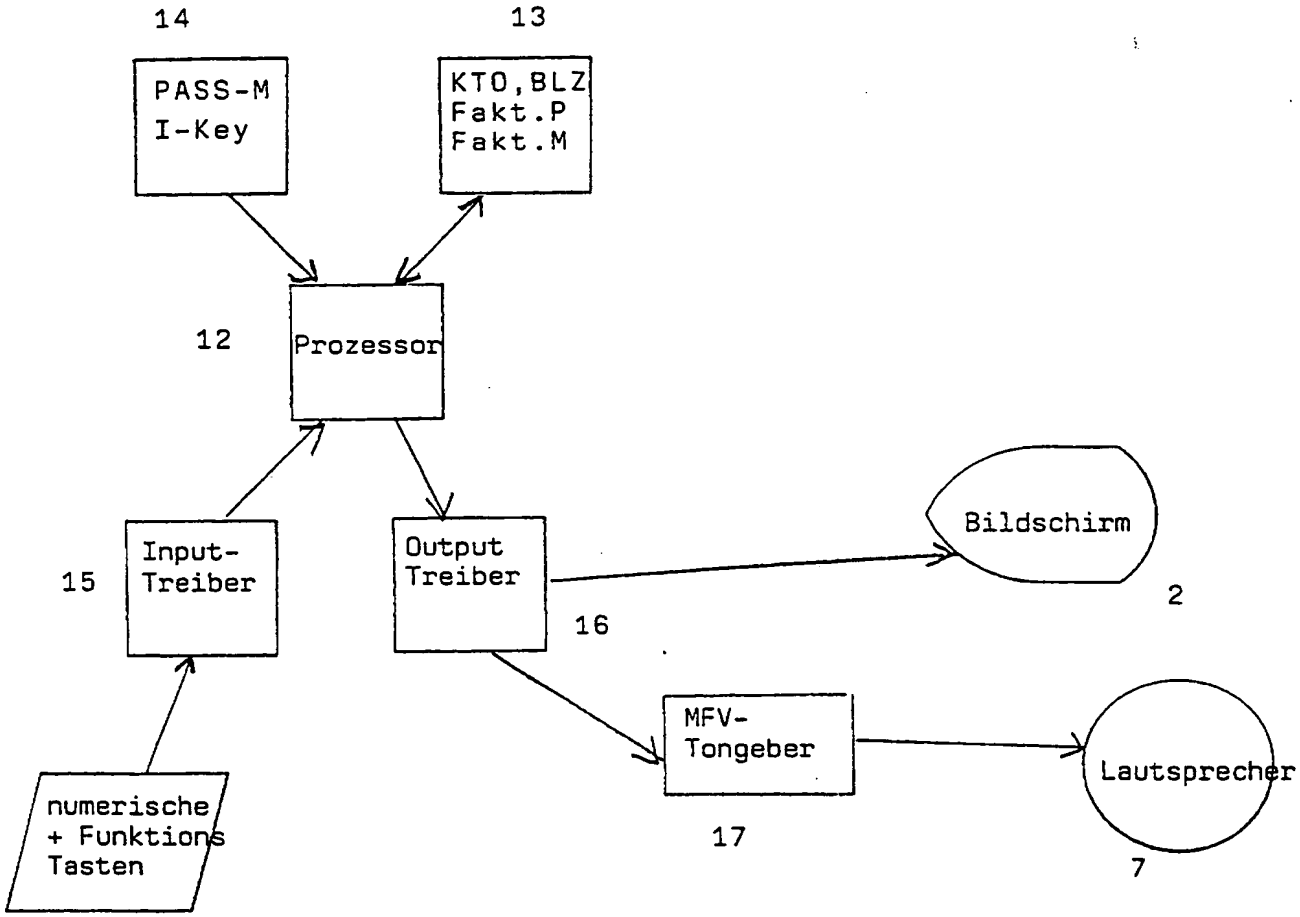


FIG. 4